UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 20-20476
Honorable David M. Lawson

ANTONIO DORAN CHANDLER,

Defendant.
_____/

OPINION AND ORDER DENYING MOTION TO SUPPRESS EVIDENCE

Defendant Antonio Chandler, charged with two counts of possessing a firearm while being an unlawful user of controlled substances, 18 U.S.C. § 922(g)(3); 21 U.S.C. § 802, has filed a motion to suppress evidence recovered in a search of his cell phone that was authorized by a search warrant. Chandler argues that the search warrant is overbroad because the supporting affidavit does not establish probable cause to search multiple application files on the smart phone or to seize more than "very narrow categories" of items, far less than the warrant authorized. Chandler contends that the search warrant, therefore, contravenes the Fourth Amendment's particularity requirement. After hearing oral argument on the motion, the Court disagrees. The search warrant, for the most part, is supported by probable cause, and the seizures were proper. The motion to suppress, therefore, will be denied.

I.

A grand jury indicted Chandler for possessing a firearm while being an unlawful user of controlled substances, contrary to 18 U.S.C. § 922(g)(3) and 21 U.S.C. § 802. In separate counts, the indictment charged that Chandler possessed a Glock 19 9mm pistol "on or about" September 9, 2020 and an Anderson Manufacturing AM-15 multi-caliber firearm "on or about" September 24, 2020. Chandler moved to suppress unspecified evidence obtained during a search of an Apple

iPhone that was seized from the defendant's pocket during his arrest. The search was authorized by a search warrant.

The investigation apparently started when government agents reviewed the defendant's Instagram account. In September 2020, ATF Agent Brett Brandon reviewed publicly available postings and profile information on the account of an Instagram user with the handle "glizzytone." Brett Brandon aff. ¶ 5, ECF No. 19-1, PageID.122. Brandon observed a photo dated June 29, 2020, which depicted the apparent owner of the account holding two pistols. *Id.* at PageID.123. Brandon also compared the likeness to a 2018 driver license photo of the defendant that was obtained from the Michigan Secretary of State, and he concluded that the person in the Instagram photo was the defendant.

Brandon continued his review of the account and observed other photos depicting firearms and apparently illegal drugs. In a photo from August 9, 2020, two Glock pistols are seen resting on a person's lap; the serial number visible on one gun was matched to a pistol reported as stolen in 2018. *Id.* at PageID.125. An Instagram "story" posted the next day depicted a "ride around" with "more then [sic] 3 glocks," and it showed two pistols under the leg of a person who was seated in an automobile. *Id.* at PageID.127. Similar photos and videos from August 14, 23, and 24, 2020, and September 16 and 21, 2020, showed persons brandishing the same and other firearms, and the defendant's face was visible in several instances. Other posts from September 12 through 19, 2020 showed the poster holding and indicating that he was about to consume Oxycodone and marijuana. *Id.* at PageID.138-142. Agent Brandon attested that he also had reviewed a cell phone seized from an "associate" of the defendant under another federal warrant and discovered text messages sent from the defendant's phone stating that the defendant recently had used "perc," which Brandon said is the street name for Percocet.

On September 24, 2020, "glizzytone" initiated a live streaming video on the Instagram account in which agents saw him apparently smoking marijuana and brandishing an assault rifle. Investigators determined the location of Chandler's phone using GPS tracking data, an arrest warrant was obtained, and Chandler shortly thereafter was pulled over and arrested. The phone at issue in this case was found in his pocket during a search incident to his arrest. Agents also obtained consent to search the home from which Chandler had emerged just before his arrest, where they found a loaded assault rifle and some quantity of marijuana.

The authorization attached to the warrant defined the scope of the search allowed as follows:

> The government is authorized to seize all information that constitutes fruits, evidence, or instrumentalities of violations 18 U.S.C. § 922(g)(3) (unlawful user of controlled substances in possession of a firearm) involving ANTONIO DORAN CHANDLER, and associates, including, but not limited to, information pertaining to the following matters:
>
> a. Any and all records showing ownership of [the] device;
>
> b. Any information showing preparatory steps taken in furtherance of the subject offenses or evidence of involvement of subject offenses;
>
> c. Any evidence relating to co-conspirators of the subject offenses;
>
> d. Evidence of use, possession, transportation, sale, distribution of firearms, including other sources of firearms, dates, places, and amounts of specific transactions;
>
> e. Evidence of use, possession, transportation, and acquisition of controlled substances, specifically marijuana, including dates, places, and amounts of specific transactions;
>
> f. Evidence indicating how and when the Target Devices were accessed or used, to determine the chronological and geographic context of access, use, and events relating to the crimes under investigation;
>
> g. Any and all incoming or outgoing communications including, but not limited to, calls and text messages, and any and all logs of such communications;
>
> h. Any and all photographs and videos relating to the subject offenses or showing preparatory steps taken in furtherance of the subject offenses;

> i. Any location information that helps reveal the whereabouts of the Subject Device and the person(s) in possession of the Subject Device;
>
> j. The identity of the person(s) who communicated with the Subject Device relating to the subject offenses, including records that help reveal their whereabouts; and
>
> k. Evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

Mot. To Suppress, Ex. A, Search Warrant Attachment B, ECF No. 19-1, PageID.157-58.

According to the government, the search warrant was executed, and agents extracted data (texts, posts, and images) establishing the defendant's use of marijuana and possessing firearms, and also information that ties the defendant to a drive-by shooting on September 9, 2020. The full extent of the extraction is not apparent from the motion papers, although in a supplement the defendant mentions that the government seized photographs, videos, text messages, call logs, and GPS location data from several iPhone applications.

The defendant concedes that the warrant affidavit set forth probable cause to believe that he had violated 18 U.S.C. § 922(g)(3) by possessing a firearm while being an illegal drug user. However, he contends that the authorization language of the warrant was unduly broad because it permitted an unrestrained sweep of the phone for electronically stored information with no apparent relationship to the documented instances of illegal gun possession on certain specific dates in June, August, and September 2020. He believes that search warrant should have cabined the iPhone search to the timeframe corresponding to the social media posts. He also argues that the search warrant was overbroad because it allowed a search for information relating to "co-conspirators," for evidence of when the firearms involved in the offense may have been unlawfully procured or used in other, unidentified crimes, and for records of "incoming and outgoing communications." He says that the affidavit does not establish probable cause for a search that

extended beyond the suspected crime (unlawful firearm possession) under investigation. And because the allegedly unlawful part of the warrant cannot be severed, he contends that the entire search warrant is invalid, and all the seized evidence should be suppressed.

II.

It is well settled that the Fourth Amendment prohibits "unreasonable searches and seizures," and that in most instance, a search is unreasonable "if it is not conducted pursuant to a warrant issued upon probable cause." *Liberty Coins, LLC v. Goodman*, 880 F.3d 274, 280 (6th Cir. 2018) (quoting U.S. Const. amend. IV and citing *Camara v. Municipal Court of City & County of San Francisco*, 387 U.S. 523, 528-29 (1967)). The parties also agree that a warrant must be obtained by police before searching a cell phone seized from the accused's person. "[In *Riley v. California*, 573 U.S. 373, 394-95 (2014)], the [Supreme] Court recognized the 'immense storage capacity' of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (citing 134 S. Ct. at 2489). That requirement nominally was satisfied in this case.

The Fourth Amendment contains a further requirement: "that a search warrant 'particularly describ[e]' the places law enforcement may search and the things they may seize." *United States v. Castro*, 881 F.3d 961, 964 (6th Cir. 2018). (quoting U.S. Const. amend. IV). Thus, "[w]arrants [both] empower and constrain" investigators to conduct the authorized search. *Ibid.* (citing *Riley*, 134 S. Ct. at 2485). The defendant now contends that this requirement was dishonored for two reasons: the search warrant allowed the police to search for and seize a broad swath of information beyond proof of the gun possession offense under investigation; and the warrant did not limit the search to the iPhone applications in which, per the affidavit, there was probable cause to suspect that the evidence might be found.

The first point is answered by *Castro*, where the court of appeals explained that "[a] warrant that empowers police to search for something satisfies the particularity requirement if its text constrains the search to evidence of a specific crime." 881 F.3d at 965 (citing *Andresen v. Maryland*, 427 U.S. 463, 480-81 (1976)). Where the warrant recites that it is based on probable cause to believe certain crimes have been committed, the designation of the offenses "serve[s] as a 'global modifier' that limit[s] the scope of the warrant to evidence of [the named offenses]." *Ibid.* This aspect of the defendant's particularity challenge is premised on a stilted reading of the affidavit at odds with the elements of the crimes alleged. Looking at the affidavit in its entirety, it is apparent that the recitation that preceded paragraphs a through k of Attachment B of the search warrant limited the authority to search the phone for evidence of violations of 18 U.S.C. § 922(g)(3). "A commonsense contextual reading" of the affidavit and search warrant defeats that aspect of the defendant's particularity challenge.

The defendant also criticizes the search warrant's lack of any temporal limitations, contending that because the social media posts referenced in the affidavit were made in June through September 2020, the search warrant should have confined the search to that timeframe. But "probable cause" is not defined so rigidly. It is not a "high bar," *Kaley v. United States*, 571 U.S. 320, 338 (2014); rather, it is established by facts — and reasonable inferences drawn for those facts — that permit "a reasonable person" to find a "fair probability" that "evidence of a crime" will be found in a particular place. *United States v. Vance*, --- F.4th ---, No. 20-5819, 2021 WL 5133250, at *5 (6th Cir. Nov. 4, 2021) (citing *Florida v. Harris*, 568 U.S. 237, 243-44 (2013)). It was reasonable for the magistrate judge to conclude from evidence of the June Instagram postings that the defendant may have documented earlier instances of his drug use and weapons possession.

The magistrate judge was not required to assume that this was the defendant's first encounter with those items.

The defendant's argument also ignores the essential elements of the charge recited in the affidavit, proof of which requires the government to establish that the defendant used drugs "regularly" and "over an extended period of time," contemporaneously with his possession of firearms. *See United States v. Bowens*, 938 F.3d 790, 793 (6th Cir. 2019) (discussing the elements of 18 U.S.C. § 922(g)(3) and quoting *United States v. Burchard*, 580 F.3d 341, 350 (6th Cir. 2009)). Thus, based on information suggesting that the defendant possessed both guns and drugs repeatedly on certain dates in June through September 2020 — which the defendant admits established probable cause to believe he had violated 18 U.S.C. § 922(g)(3) — the authorization for the search fairly encompassed information tending to show that the defendant possessed and used narcotics both "with regularity," and "over an extended period of time" during that operative time frame. The comprehensive search for evidence of such possession proximate to that time frame was not, contrary to the defendant's position, beyond the concededly sufficient showing of probable cause for the charged crime.

The defendant's second argument — that the search warrant did not particularly describe the "places" on the cell phone that could be searched — is based primarily on the now-vacated panel opinion in *United States v. Morton*, 984 F.3d 421 (5th Cir. 2021), *reh'g en banc granted*, *opinion vacated*, No. 19-10842, 2021 WL 1990794 (May 18, 2021). The panel held that an affidavit for a warrant to search a cell phone must establish probable cause for "each place to be searched" on the device, such as the subject's "contacts, his call logs, his text messages, and his photographs." *Id.* at 427. The panel drew its reasoning from the Supreme Court's observations in *Riley* about the comprehensive nature of information stored by the typical cell phone user — from

which "the sum of an individual's private life can be reconstructed," *Riley*, 573 U.S. at 395 — and that "certain types of data" on cellphones are "qualitatively different" from other types, *ibid.* *Morton*, 984 F.3d at 426. The panel believed that its holding naturally flowed from the Fourth Amendment's requirement that search warrants must "particularly describe the place to be searched," U.S. Const. Am. IV, and that allowing all contents of a cell phone to be searched in every case would be like the "reviled general warrant" that historically "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," *Riley*, 573 U.S. at 403, which the Amendment was intended to prohibit, *Morton*, 984 F.3d at 426 n.4.

That reasoning is somewhat in tension with a case decided by the Sixth Circuit under a plain-error review that analogized a cell phone search to a search of a personal computer. *See United States v. Bass*, 785 F.3d 1043, 1049-50 (6th Cir. 2015). The court observed that "most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers" are rejected because "criminals can — and often do — hide, mislabel, or manipulate files to conceal criminal activity such that a broad, expansive search of the computer may be required." *Ibid.* (cleaned up). But that reasoning does not give due consideration to the Supreme Court's apprehension that discrete cell phone applications are distinct and may harbor separate and unrelated data sets and trigger unique privacy concerns. *See Riley*, 573 U.S. at 395-96 ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular

building."). It also does not give full effect to the established constitutional principles that the court recited, namely, that "[t]o justify a search, the circumstances must indicate why evidence of an illegal activity will be found in a 'particular place,'" and that the search warrant affidavit "must establish a nexus between the place to be searched and things to be seized, such that there is a substantial basis to believe that the things to be seized will be found in the place searched." *Bass*, 785 F.3d at 1049 (quoting *Illinois v. Gates,* 462 U.S. 213, 238 (1983), and *Ellison v. Balinski,* 625 F.3d 953, 958 (6th Cir. 2010)).

The Supreme Court recognized the impracticality of directly comparing searches for digital data to searches for items in the physical world. *Riley*, 573 U.S. at 398-400. But the Court itself drew an analogy to physical searches when describing the limitations of certain warrantless encounters. *See id.* at 402 ("In *Chadwick,* for example, the Court held that the exception for searches incident to arrest did not justify a search of the trunk at issue, but noted that 'if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without opening the luggage.'" (citing *United States v. Chadwick*, 433 U.S. 1, 15, n.9 (1977)). Following that lead, it is appropriate to view a smart phone as a repository of discrete caches of information, which are "places" that can be searched if probable cause supports the intrusion. *See United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (allowing a search of a computer under a warrant to be "as extensive as reasonably required to locate the items described in the warrant *based on probable cause*") (emphasis added). However, if the affidavit does not establish probable cause to find that information reasonably may be found in a particular data file or category of files, the warrant may not authorize the search of those files, folders, or applications.

In this case, the affidavit did establish probable cause to search for information in some but not all the "places" on the defendant's cell phone. One must remember that "[t]he Fourth Amendment does not require probable cause to believe evidence will conclusively establish a fact before permitting a search, but only probable cause to believe that the evidence sought will aid in a particular apprehension or conviction." *Peffer v. Stephens*, 880 F.3d 256, 263 (6th Cir. 2018) (quotation marks omitted). Ownership, registration, and usage data for the phone would aid the government in establishing that the phone belonged to the defendant and was used by him, and that it was used to post information to the "glizzytone" Instagram account, thus bolstering the proof of identity and helping to show that the person in the photos was the defendant. Information tending to show both possession and procurement of firearms, and the times and dates when such occurred, would be relevant to proving the basic elements of the crime. Information about when and how the defendant procured and used both firearms and drugs also would aid in establishing that he did so knowingly, and that his exhibitions with firearms and drugs in hand were not mere happenstance. Communications with other persons relating to gun and drug possession would aid in establishing that the defendant used drugs regularly, over an extended period, and contemporaneously with his possession of firearms. Those communications also likely would aid the government in locating witnesses who might have further personal knowledge of the defendant's charged conduct. Geographic location and origination data associated with all of the above would be essential to establishing venue and jurisdiction in this Court for any potential charges. All of that information certainly would advance the investigation of the charged offenses.

A commonsense reading of the affidavit supports the conclusion that this information would be found in the social media applications on the smart phone, the text message applications, and the GPS tracking applications. The same can be said for the files that store photographs,

voicemail messages, call logs, and subscriber data. But it is not readily apparent, and the government has not explained, how the facts in the affidavit establish probable cause to search contact lists, phone books, document files, or browsing history, which are listed in subparagraph k of Attachment B to the search warrant. However, the defendant has not alleged that the government agents used the search warrant to access those files or seize any information. Moreover, subparagraph k's language does not "doom the entire warrant." *Castro*, 881 F.3d at 965 (quoting *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001)). In such cases, "[t]he remedy is to sever the offending phrase from the warrant, suppress any evidence collected under it, and admit the evidence collected under the valid portions that remain." *Ibid.*

The defendant has not pointed to any evidence seized under subparagraph k of the warrant. And the seized evidence described in the government's brief falls within the warrant's valid authorization.

The government also invokes the so-called "good faith" exception to the exclusionary rule described in *United States v. Leon*, 468 U.S. 897, 905 (1984). However, because the defendant has not identified any evidence that was seized improperly under the search warrant, the Court need not address that argument.

III.

Although not all the information particularly described by the search warrant was subject to seizure upon probable cause, the warrant's overbreadth does not render it invalid in total, and the defendant has not identified any evidence seized under any of the warrant's offending provisions.

Accordingly, it is **ORDERED** that the defendant's motion to suppress evidence (ECF No. 19) is **DENIED**.

s/David M. Lawson
DAVID M. LAWSON
United States District Judge

Dated: November 10, 2021